

10/523583
PCT/EP 02/11420



Europäisches
Patentamt

European
Patent Office

Office européen
des brevets

REC'D 28 NOV 2002

WIPO

PCT

Bescheinigung

Certificate

Attestation

Die angehefteten Unterla-
gen stimmen mit der
ursprünglich eingereichten
Fassung der auf dem näch-
sten Blatt bezeichneten
europäischen Patentanmel-
dung überein.

The attached documents
are exact copies of the
European patent application
described on the following
page, as originally filed.

Les documents fixés à
cette attestation sont
conformes à la version
initialement déposée de
la demande de brevet
européen spécifiée à la
page suivante.

Patentanmeldung Nr. Patent application No. Demande de brevet n°

02016883.7

**PRIORITY
DOCUMENT**
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

R C van Dijk

DEN HAAG, DEN
THE HAGUE,
LA HAYE, LE

21/11/02

BEST AVAILABLE COPY



Europäisches
Patentamt

European
Patent Office

Office européen
des brevets

Blatt 2 der Bescheinigung
Sheet 2 of the certificate
Page 2 de l'attestation

Anmeldung Nr.:
Application no.:
Demande n°: 02016883.7

Anmeldetag:
Date of filing: 30/07/02
Date de dépôt:

Anmelder:
Applicant(s):
Demandeur(s):
mega-tel AG/SA
3073 Gümliigen
SWITZERLAND

Bezeichnung der Erfindung:
Title of the invention:
Titre de l'invention:

Identifikation eines Benutzers eines Mobilterminals

In Anspruch genommene Priorität(en) / Priority(ies) claimed / Priorité(s) revendiquée(s)

Staat:
State:
Pays:

Tag:
Date:
Date:

Aktenzeichen:
File no.
Numéro de dépôt:

Internationale Patentklassifikation:
International Patent classification:
Classification internationale des brevets:

/

Am Anmeldetag benannte Vertragsstaaten:
Contracting states designated at date of filing:
Etats contractants désignés lors du dépôt:

AT/BE/CH/CY/DE/DK/ES/FI/FR/GB/GR/IE/IT/LI/LU/MC/NL/PT/SE/TR

Bemerkungen:
Remarks:
Remarques:

Identifikation eines Benutzers eines Mobilterminals

- Die vorliegende Erfindung bezieht sich auf ein Verfahren zur Identifizierung eines Benutzers eines Mobilterminals und auf ein Verfahren zur Generierung einer Aktionsberechtigung für einen Benutzer eines Mobilterminals. Bei dem Mobilterminal kann es sich dabei insbesondere um ein Mobiltelefon, einen „Personal Digital Assistent“ (PDA) oder dergleichen handeln. Bei den betreffenden Aktionen handelt es sich allgemein um Vorgänge, die eine Berechtigung und/oder Identifizierung erfordern, wie zum Beispiel Zahlungsvorgänge, personenspezifisches Passieren von Türen oder Schranken oder um Stimmabgaben bei einer Wahl. Die Erfindung bezieht sich weiterhin auf ein System zur Durchführung des erfindungsgemäßen Verfahrens sowie auf ein Softwareprogramm, durch das eine Implementierung des erfindungsgemäßen Verfahrens möglich ist.
- 20 Die meisten Sicherheitssysteme im Zusammenhang mit Kreditkarten, Zahlkarten, Electronic-Banking oder Zutrittskontrollen für Räumlichkeiten oder auch Computer-Netzwerke beruhen auf statischen Daten, wie zum Beispiel Kreditkartennummern, Daten auf Magnetstreifen oder Chips, Fotos, Nummern einer Streichliste in gedruckter Form, Badge oder Token. Die damit verbundenen Risiken, beispielsweise bei Entwendung einer Kreditkarte sind offensichtlich und allgemein bekannt.
- 30 Sicherheitssysteme, die auf dynamischen Daten beruhen, werden beispielsweise bei Zutrittskontrollen, bei Netzwerkanmeldungen an einem Personal Computer oder beim E-Banking eingesetzt. Vorzugsweise werden hierfür Prozessoren verwendet, die in regelmäßigen zeitlichen Abständen mittels spezieller Algorithmen dynamisch Werte für Codenummern
- 35

generieren. Diese werden dann bei einer Anmeldung oder einem Zutritt oder dergleichen mit Referenzwerten verglichen. Bei Übereinstimmung wird eine Freigabe ausgelöst.

5

Neben diesen bekannten „SecurID-Komponenten“, wie sie beispielsweise von „RSA Security“ vertrieben werden, gibt es in letzter Zeit auch vermehrt PDAs, „Organizers“ und dergleichen sowie Mobiltelefone, die in der Lage sind, derartige Funktionen wahrzunehmen.

Eine Unsicherheitskomponente ist in diesem Zusammenhang beim Stand der Technik, dass sicherheitsrelevante Daten, wie zum Beispiel die Nummer einer Kreditkarte an eine an der Aktion beteiligten Partei, beispielsweise dem Betreiber eines Supermarktes übermittelt werden müssen.

Beispielsweise werden sicherheitsrelevante Daten einer Kreditkarte von einem Lesegerät an einem Zahlungsterminal erfasst, um eine Transaktion zu initialisieren. Dabei werden die relevanten Daten übermittelt, kontrolliert, freigegeben und die Zahlungsaktion terminiert. Die Daten auf der verwendeten Kreditkarte sind statisch. Sie werden auf dem Beleg, der zur Unterschrift vorgelegt wird, mehr oder weniger ungeschützt ausgewiesen.

25

Einige Unternehmen sind dazu übergegangen, die letzten vier Ziffern beim Ausdruck auf dem Beleg zu trunkieren. Dennoch können missbräuchliche Anwendungen nicht ausgeschlossen werden, sofern die Karte dem Vertragspartner vorübergehend zugänglich gemacht wird.

30

Der vorliegenden Erfindung liegt die Aufgabe zugrunde, eine Technik bereitzustellen, mit der es ermöglicht wird, einen Benutzer eines Mobilterminals, insbesondere eines Mobiltelefons, zu identifizieren und/oder für ihn eine

35

Berechtigung für die Ausführung einer Aktion zu generieren, wobei besonders hohe Sicherheit zu gewährleisten ist.

5 Diese Aufgabe wird erfindungsgemäß durch die Merkmale der unabhängigen Ansprüche gelöst. Die abhängigen Ansprüche bilden den zentralen Gedanken der Erfindung in besonders vorteilhafter Weise weiter.

10 Gemäß der Erfindung wird für einen Benutzer eines Mobilterminals, insbesondere eines Mobiltelefons, PDA's oder dergleichen eine Berechtigung für eine Aktion erzeugt. Dabei wird in einem ersten Schritt von dem Mobilterminal über eine Luftschnittstelle - beispielsweise mittels einer „Short Message Service“ (SMS)-Nachricht eine Anfrage an ein
15 Identifikationsmodul gesendet. Das Identifikationsmodul ist dabei von dem Benutzer unabhängig.

In einem folgenden Schritt wird von dem Identifikationsmodul eine Aktions-Codenummer erzeugt und an
20 das Mobilterminal gesendet. Auf den Empfang der Aktions-Codenummer hin wird von dem Mobilterminal eine persönliche Identifikationsnummer (PIN) über eine Luftschnittstelle an das Identifikationsmodul gesendet. Durch den letztgenannten Schritt aktiviert der Benutzer die entsprechende
25 Aktionsberechtigung. Das Verfahren ist dadurch gekennzeichnet, dass die Aktions-Codenummer eine zeitlich begrenzte Gültigkeit besitzt. Die Dauer der zeitlichen Begrenzung kann dabei je nach spezieller Anforderung, die durch die betreffende Aktion gegeben sind, gewählt werden.

30 Alternativ wird im letzten Schritt vom Mobilterminal oder von einem anderen Sendegerät - beispielsweise ein an das Internet angeschlossener Personal Computer (PC) - eine PIN an ein Aktionsterminal gesendet. Dabei besteht eine
35 Verbindung zwischen dem Aktionsterminal und der Aktion, für

die der Benutzer des Mobilterminals zu Beginn des Verfahrens eine Berechtigung anfordert. Die Verbindung ist dadurch gegeben, dass mittels des Aktionsterminals Vorgänge auslösbar sind, die für die gewünschte Aktion nötig sind.

~~5 Beispielsweise kann durch das Aktionsterminal eine Tür~~
oder Schranke geöffnet werden oder eine bargeldlose Zahlung ausgelöst werden.

10 Durch diese Schritte wird es möglich, dass bei besonders hoher Sicherheit der Betreiber des Aktionsterminals keine personenspezifischen Daten des Benutzers erhält, aber dennoch die gewünschte Aktion durchgeführt werden kann.

15 Vorteilhaft ist es, wenn durch die Übersendung der PIN von dem Benutzer des Mobilterminals die Aktionsberechtigung terminiert wird. Dies stellt eine zusätzliche Sicherheitsmassnahme dar.

20 Vorteilhaft ist es außerdem, wenn die Aktions-Codenummer nur einmal gültig ist. Möglich ist auch eine mehrmalige Gültigkeit der Aktions-Codenummer, wobei allerdings die maximale Anzahl der Aktionsberechtigungen für eine Aktions-Codenummer beschränkt ist. Dadurch wird eine besonders hohe Sicherheit bei der Vergabe einer Aktionsberechtigung
25 erzielt.

Weiterhin ist es vorteilhaft, wenn die Kommunikation
zwischen dem Mobilterminal und dem Identifikationsmodul
zumindest teilweise mittels eines Datenkanals, wie zum...
30 Beispiel einer SMS-Nachricht des GSM-Standards erfolgt. Dadurch werden keine Nutzkanäle belegt. Außerdem ist dies aufgrund der weiten Verbreitung des SMS-Dienstes günstig. Schließlich ist ein derartiger Datenkanal auch
störungssicherer als ein Nutz- beziehungsweise Sprachkanal.

Auch ist es vorteilhaft, wenn zur Kommunikation zwischen dem Mobilterminal und dem Identifikationsmodul Daten verwendet werden, die aus einem Speicher, beispielsweise in Form einer „Subscriber Identity Module“ (SIM) Karte in dem Mobilterminal ausgelesen werden.

Durch eine Verschlüsselung der Kommunikation zwischen dem Mobilterminal und dem Identifikationsmodul wird die Sicherheit weiter erhöht.

10

Werden Informationen bezüglich der von dem Benutzer gewünschten Aktion in einem Speicher des Mobilterminals abgelegt, können sie von berechtigten Personen ausgelesen und/oder zu einem anderen Gerät übertragen werden.

15

Beispielsweise eignet sich das Verfahren in besonderer Weise für die Abwicklung eines bargeldlosen Zahlungsvorganges.

20 Bei dem Aktionsterminal kann es sich beispielsweise um das Terminal eines Zahlungsadressaten, zum Beispiel eines Supermarkt-Betreibers, handeln.

25 Mit dem Aktionsterminal sind in diesem Fall beispielsweise Vorgänge einer Kasse in einem Supermarkt auslösbar.

Mit weiteren vorteilhaften Ausgestaltungen eines Aktionsterminals kann beispielsweise eine Türe geöffnet oder ein Ticket gedruckt werden.

30

Schließlich kann es sich bei der gewünschten Aktion um eine Stimmabgabe des Benutzers bei einer Wahl oder Abstimmung handeln.

35 Gemäß einem weiteren Aspekt der Erfindung wird ein Benutzer

eines Mobilterminals, insbesondere eines Mobiltelefons oder dergleichen gegenüber einem Identifikationsadressaten identifiziert. Dazu wird ein Identifikationsmodul verwendet, das sowohl von dem Benutzer als auch von dem

5 Identifikationsadressaten unabhängig ist. Außerdem wird ein Terminal des Identifikationsadressaten verwendet.

In einem ersten Schritt wird von dem Benutzer unter Verwendung des Mobilterminals eine Anforderung für eine
10 Identifizierung gegenüber dem Identifikationsadressaten an das Identifikationsmodul gesendet. In einem weiteren Schritt wird von dem Identifikationsmodul eine Berechtigungs-Codenummer erzeugt. In einem folgenden Schritt wird die Berechtigungs-Codenummer von dem
15 Identifikationsmodul an das Mobilterminal gesendet. Außerdem wird die Berechtigungs-Codenummer an das Terminal des Identifikationsadressaten gesendet.

Schließlich wird von dem Mobilterminal eine PIN an das
20 Identifikationsmodul gesendet. Durch den letztgenannten Schritt aktiviert der Benutzer die Identifizierungs-Anforderung.

Das Verfahren ist dadurch gekennzeichnet, dass die
25 Übersendung der Berechtigungs-Codenummer an das Terminal des Identifikationsadressaten zumindest teilweise über eine Luftschnittstelle erfolgt. Beispielsweise kann das Terminal über ein GSM-Modul ansteuerbar sein.

30 Alternativ kann im letzten Schritt die Übersendung einer PIN von dem Benutzer mit einem Sendegerät an das Terminal des Identifikationsadressaten erfolgen. Dabei wird ein Telekommunikationsnetz, beispielsweise das Internet verwendet. Als Sendegerät eignet sich in diesem Fall
35 beispielsweise ein PC des Benutzers.

Vorteilhaft ist es, wenn die Gültigkeit der Identifizierungs-Codenummer zeitlich begrenzt ist.

- 5 Weiterhin ist es vorteilhaft, wenn die Identifizierungs-Codenummer nur einmal gültig ist. Alternativ kann die Identifizierungs-Codenummer begrenzt oft gültig sein.

- 10 Durch die beiden letztgenannten Merkmale wird die Sicherheit des Verfahrens besonders erhöht.

- 15 Weiterhin ist es vorteilhaft, wenn die Identifizierung, die von dem Benutzer zu Beginn des Verfahrens angefordert wird, durch die Übersendung der PIN aktiviert beziehungsweise terminiert wird.

- 20 Gemäß einem weiteren Aspekt der Erfindung erfolgt eine Identifizierung eines Benutzers eines Mobilterminals gegenüber einem Identifikationsadressaten unter Zuhilfenahme eines Mobilterminals, eines davon unabhängigen Identifikationsmoduls und eines Terminals des Identifikationsadressaten.

- 25 Das Verfahren weist dabei folgende Schritte auf: Zunächst wird von dem Benutzer eine Identifikations-Anforderung von dem Mobilterminal über eine Luftschnittstelle an das Identifikationsmodul gesendet. In einem nächsten Schritt wird von dem Identifikationsmodul eine Identifizierungs-Codenummer generiert. In einem folgenden Schritt wird von 30 dem Identifikationsmodul die Identifizierungs-Codenummer über eine Luftschnittstelle an das Mobilterminal gesendet. Außerdem wird die Identifizierungs-Codenummer von dem Identifikationsmodul über eine Luftschnittstelle an das Terminal des Identifikationsadressaten gesendet.

Schließlich wird von dem Benutzer eine PIN von dem Mobilterminal an das Identifikationsmodul gesendet. Mit dem letztgenannten Schritt aktiviert der Benutzer die angeforderte Identifikation.

5

Das Verfahren ist dadurch gekennzeichnet, dass die Gültigkeit der Identifizierungs-Codenummer zeitlich begrenzt ist. Dadurch wird besonders hohe Sicherheit erzielt.

10

Alternativ kann die Übersendung der PIN von dem Benutzer des Mobilterminals über ein Telekommunikationsnetz, beispielsweise das Internet mittels eines Sendegerätes, beispielsweise einem PC direkt an das Terminal des Identifikationsadressaten erfolgen. Die persönliche Identifikationsnummer ist dabei vorab zwischen dem Benutzer und dem Identifikationsadressaten vereinbart.

15

Vorteilhaft ist es, wenn die Identifizierungs-Codenummer nur einmal gültig ist. Alternativ kann die Anzahl der Gültigkeiten der Identifizierungs-Codenummer nach oben beschränkt sein. Auch hierdurch wird eine besonders hohe Sicherheit erzielt.

20

Weitere Merkmale, Vorteile und Eigenschaften sollen nunmehr anhand einer detaillierten Beschreibung von Ausführungsbeispielen und bezugnehmend auf die Figuren der beigefügten Zeichnungen erläutert werden. Es zeigen:

25

Fig. 1 grundlegendes Ablaufschema des erfindungsgemäßen Verfahrens;

30

Fig. 2 Ablaufschema des erfindungsgemäßen Verfahrens im Falle einer Anwendung im Rahmen einer Stimmabgabe bei einer Wahl oder Abstimmung;

35

Fig. 3 Datenflussplan - Grundmodul;

Fig. 4 Datenflussplan - Öffnung einer Zugangsschleuse;

5

Fig. 5 Datenflussplan - Zahlung mit Kredit- oder
Debitkarte;

Fig. 6 Datenflussplan - Übermittlung einer E-Banking
Streichliste;

10

Fig. 7 Datenflussplan - Bargeldbezug am Geldautomaten;

Fig. 8 Datenflussplan - Erstellung eines Tickets im
E-Ticketing; und

15

Fig. 9 Datenflussplan - Übermittlung eines Zugriffs-
Passwortes.

20 Fig. 1 zeigt schematisch die zeitliche Abfolge des
erfindungsgemäßen Verfahrens. Insgesamt betrachtet läßt
sich das Verfahren in zwei Abschnitte untergliedern: eine
„Vorauthorisierung“ 10 und eine „Terminierung“ 20.

25 Vorauthorisierung

Bei der Vorauthorisierung 10 fordert in einem ersten
Schritt 5 ein Benutzer 1 eines Mobiltelefons über Menü-
Steuerung bei dem Identifikationsmodul 2 einen Code an.

30 Dieser Code kann beispielsweise mit „Aktions-Codenummer“,
„Berechtigungs-Codenummer“, „Identifizierungs-Codenummer“
oder dergleichen bezeichnet werden. Im Folgenden wird
hierfür der Ausdruck „Transaktionscode“ (TRX) verwendet.

35 Zusammen mit dieser Nachricht werden außerdem

aktionsspezifische Angaben übermittelt. Beispielsweise kann mitgeteilt werden, auf welche Aktion sich der TRX beziehen soll. Beispiele für diese Aktionen sind:

-
- 5 • Durchgang des Benutzers durch eine kontrollierte Türe oder Schranke,
 - Zahlungsvorgang mit einer Kredit- oder Debitkarte,
 - Erhalt einer E-Banking Streichliste für den Benutzer,
 - Bargeldbezug durch den Benutzer von einem Geldautomaten,
 - 10 • Kauf eines „Electronic Ticket“ im Fernverkehr,
 - Zugriff des Benutzers auf eine Seite des World Wide Web,
 - Teilname des Benutzers an einem „E-Voting“.

Je nach Aktion werden außerdem weitere aktionsrelevante
 15 Daten übermittelt, wie beispielsweise die Identifikation der SIM-Karte, eine Berechtigung zur Anfrage, eine PIN-Nummer, die „Cell Identification“, ein Betrag einer Zahlung etc.

20 Die Anforderung 5 erfolgt beispielsweise mittels des SMS-Dienstes über ein Telekommunikationsnetz eines Netzbetreibers nach dem GSM Standard. Durch den entsprechenden Netzprovider wird die Nachricht an das Identifikationsmodul 2 drahtlos übermittelt.

25

~~In einem zweiten Schritt 6 wird in dem Identifikationsmodul~~
 2 die Anforderung des Benutzers registriert und die in der Anforderung 5 übermittelten Daten werden dort verifiziert.

30 Bei Übereinstimmung des Profils der übermittelten Daten mit im Identifikationsmodul 2 vorliegenden Vergleichsdaten wird daraufhin von dem Identifikationsmodul 2 - genauer gesagt durch einen Server des Identifikationsmoduls 2 - ein einmal gültiger TRX generiert, der mit einer Zeitbeschränkung

versehen ist. Die Zeitbeschränkung kann dabei beliebig fixiert sein. Beispielsweise kann die Zeitbeschränkung 15 Minuten betragen. Die Dauer der Zeitbeschränkung kann in Abhängigkeit der Art der Aktion gewählt sein.

5

In einem weiteren Schritt 7 wird dann der so generierte TRX an den Benutzer 1 des Mobiltelefons und an eine an der Aktion beteiligte weitere Partei oder gegebenenfalls weitere Parteien übermittelt. Bei dieser weiteren Partei
10 kann es sich beispielsweise handeln um

- ein Terminal, das mit einer Zutrittsschleuse verbunden ist,
- ein Kassenterminal für Kredit- und Debitkarten,
- 15 • ein Terminal einer Bank, durch das eine Streichliste für E-Banking generiert werden kann,
- ein Terminal, das mit einem Geldautomaten für Bargeldbezug verbunden ist,
- ein Terminal an einer Fahrkartenverkaufsstelle für das
20 „Electronic Ticketing“ im Fernverkehr,
- einen Internet-Server,
- einen Server einer Behörde, durch die ein „E-Voting“ durchgeführt wird.

25 In Fig. 1 ist schematisch als Repräsentant für eine weitere Partei ein Terminal 3 dargestellt.

Die Übermittlung an die weitere Partei kann wiederum über eine Luftschnittstelle erfolgen. Beispielsweise kann ein
30 Terminal 3 der weiteren Partei über ein GSM-Modul ansteuerbar sein.

Als zusätzliche Sicherheitseinrichtung kann bei diesem Schritt ein Sicherheitscode übermittelt werden, durch den

die Provenienz des TRX vom Identifikationsmodul bestätigt wird.

Damit ist die Vorauthorisierung abgeschlossen.

5

Terminierung

Bei der Terminierung 20 wird von dem Benutzer 1 des Mobiltelefons eine Nachricht an das Identifikationsmodul 2
10 gesendet. Dabei kann es sich beispielsweise um eine PIN handeln. Es ist auch möglich, hierfür eine andere, zwischen dem Benutzer 1 des Mobiltelefons und dem Betreiber des Identifikationsmoduls 2 speziell vereinbarte Nachricht zu verwenden.

15

Im Identifikationsmodul 2 wird daraufhin die Nachricht auf Richtigkeit beziehungsweise Gültigkeit geprüft.

Im Fall der Gültigkeit wird dann seitens des
20 Identifikationsmoduls 2 mittels Nachrichtenübermittlung an die weitere Partei die Aktionsberechtigung aktiviert und die vom Mobiltelefon angeforderte Aktion kann erfolgen.

Die Nachrichtenübermittlung von dem Identifikationsmodul 2
25 an die weitere Partei 3 kann dabei über eine Luftschnittstelle erfolgen. Beispielsweise kann ein ~~Terminal der weiteren Partei 3 von dem Identifikationsmodul~~
über ein GSM-Modul angesteuert werden.

30 Mit dieser Nachricht wird seitens des Mobiltelefons das Verfahren terminiert und dadurch die Aktionsberechtigung aktiviert. Beispielsweise können dadurch folgende Vorgänge ausgelöst werden:

35 • Eine Zugangstüre öffnet sich,

- Ein Zahlungsvorgang mit einer Kredit- oder Debitkarte erfolgt,
- Ein Geldautomat gibt Geld aus,
- Ein „Electronic Ticket“ wird erstellt.

5

Alternativ kann bei der Terminierung von dem Benutzer 1 des Mobiltelefons eine Nachricht 8' direkt an die weitere Partei 3 gesendet werden. Diese Nachricht beinhaltet neben der TRX
10 einen weiteren Code, beispielsweise in Form einer „Applikations-PIN“, der zwischen dem Benutzer 1 des Mobiltelefons und der weiteren Partei 3, beispielsweise einem „Applikationsbetreiber“, speziell hierfür vereinbart ist.

15

Die Übertragung der Nachricht 8' muss nicht mittels des Mobiltelefons erfolgen. Sie kann beispielsweise alternativ von einem PC des Benutzers 1 über das Internet auf einen Server eines Applikationsbetreibers übermittelt werden.
20 Beispielsweise kann es sich dabei um eine Nachricht nach dem „File Transfer Protocol“ (FTP) handeln.

Auf jeden Fall wird bei der Terminierung 20 durch den Benutzer 1 die Aktionsberechtigung aktiviert und der vom
25 Benutzer 1 gewünschte beziehungsweise angeforderte Vorgang kann durchgeführt werden.

Beispielsweise kann es sich bei einem Applikationsbetreiber um die Behörde einer Gemeinde handeln, die ein E-Voting
30 durchführt. In diesem Fall kann bei der Terminierung der Benutzer 1 seine Stimmabgabe für das E-Voting zusammen mit der entsprechend zwischen dem Benutzer 1 und der Gemeinde vereinbarten Applikations-PIN mittels FTP über das Internet an die Gemeinde senden.

Ein weiteres Beispiel für einen Applikationsbetreiber ist eine Bank. Beispielsweise kann der Benutzer 1 (im Schritt 5) bei der Bank eine Streichliste für E-Banking anfordern.

-
- 5 Im Schritt 8' sendet dann der Benutzer 1 zusammen mit der TRX den zwischen dem Benutzer 1 und der Bank vereinbarten „Applikations-PIN“. Dies kann beispielsweise so eingerichtet sein, dass der Benutzer auf diese Weise Zugriff auf eine geschützte Web-Seite der Bank erhält, auf
10 der sich die gewünschte Streichliste befindet.

- Vorteilhaft an dem angegebenen Verfahren ist dabei insbesondere, dass an die weitere Partei keine sicherheitsrelevanten Daten des Benutzers 1 geleitet werden
15 müssen.

- Möglich ist auch der Fall, dass das Identifikationsmodul 2 und die weitere Partei 3 identisch sind. In diesem Fall erübrigt sich offensichtlich bei Schritt 7 die optionale
20 Übermittlung der TRX von dem Identifikationsmodul an die weitere Partei 3.

- Im Folgenden soll anhand von Fig. 2 am Beispiel eines E-Voting das erfindungsgemäße Verfahren dargestellt werden.
25

- Bei der Durchführung einer Abstimmung oder Wahl mit Hilfe ~~des erfindungsgemäßen Verfahrens erfolgt zunächst in einem~~
ersten Teil ein „Download der Abstimmungsunterlagen“ und anschließend in einem zweiten Teil die eigentliche
30 Abstimmung. Sowohl in Teil Eins als auch in Teil Zwei erfolgt dabei jeweils ein separater Durchlauf des erfindungsgemäßen Verfahrens.

-
- 35 ~~Zur Vorbereitung wird zunächst von der entsprechenden~~
Behörde 30 einer Gemeinde mittels Brief ein

wahlberechtigter Benutzer 1 angeschrieben. Dieser Brief beinhaltet eine Anleitung zur Initialisierung des Mobiltelefons für die E-Voting Funktion und persönliche Zugangsinformationen, sowie eine Zugangsanleitung.

5

In einem weiteren Schritt werden von der Behörde Abstimmungsunterlagen und entsprechendes Informationsmaterial bereitgestellt. Eingetragene E-Voter benötigen dabei keine Unterlagen in Briefform.

10

Nun fordert im Schritt 50 des ersten Teils der Benutzer 1 mittels SMS-Nachricht an das Identifikationsmodul 3 einen TRX für das „E-Voting-Download“ an. Diese Nachricht wird vom Benutzer 1 durch Senden einer Applikations-PIN

15 bestätigt.

In einem nächsten Schritt 60 wird im Server des Identifikationsmoduls 3 die erhaltene Nachricht durch Verifizierung der Anfrage und Überprüfung der Autorisierung des Zugriffs bearbeitet und bei Gültigkeit ein einmal gültiger TRX für das E-Voting-Download generiert. Dieser TRX ist dabei mit einer fixen Zeitbeschränkung versehen.

20

Im folgenden Schritt 70 wird dieser TRX zusammen mit dem entsprechenden Zeitlimit für die Gültigkeit des TRX per SMS-Nachricht von dem Identifikationsmodul sowohl an den Benutzer 1, als auch an die Behörde 30 gesendet. Die Behörde hat für diesen Zweck ein Terminal mit einem GSM-Modul.

30

Im nächsten Schritt 80 kann der Benutzer 1 mittels PC und Internet nach Eingabe von TRX und einer Applikations-PIN das Abstimmungsmaterial vom Server der Behörde auf seinen PC herunterladen. Damit ist der erste Teil beendet.

35

Im zweiten Teil fordert der Benutzer 1 zunächst einen (weiteren) TRX für die Stimmabgabe beim Identifikationsmodul 3 per SMS-Nachricht an 500. Diese Anforderung wird wiederum per PIN (entweder dieselbe PIN
5 wie im ersten Teil oder eine andere PIN) bestätigt.

Im Schritt 600 wird durch das Identifikationsmodul 2 durch Verifizierung und Überprüfung der Autorisierung bearbeitet. Bei Gültigkeit wird ein TRX für die Stimmabgabe generiert.
10 Dieser TRX ist nur für einen bestimmten Zeitraum und nur einmalig gültig.

Im Schritt 700 wird der TRX für die Stimmabgabe an den Benutzer 1 und die Behörde 30 gesendet.
15

Im Schritt 800 sendet der Benutzer 1 den TRX für die Stimmabgabe zusammen mit einer Applikations-PIN mittels PC und Internet - beispielsweise per FTP - an die Behörde 30.
20 Schließlich kann von der Behörde 30 mittels SMS-Nachricht an den Benutzer 1 eine Bestätigung über den Eingang der Stimmabgabe erfolgen. Gleichzeitig kann durch die Behörde eine Sperre für persönliche und/oder briefliche Stimmabgabe des Benutzers erfolgen.
25

Die Auswertung der Stimmen von E-Votern kann bei der Behörde 30 mittels eines Rechners erfolgen.
30

Durch die ortsunabhängige und zeitlich besonders flexible Gestaltungsmöglichkeit der Stimmabgabe gemäß der Erfindung kann eine Zunahme der Wahl- beziehungsweise Abstimmungsbeteiligung erwartet werden.

35 In den Figuren 3 bis 11 sind erfindungsgemäße

Datenflusspläne für Abläufe aus Sicht eines Benutzers eines Mobiltelefons dargestellt. In diesem Ausführungsbeispiel wird das Verfahren auf mehrere Module angewendet, die sich jeweils auf verschiedene Aktionen beziehen.

5

Fig. 3 zeigt das Grundmodul. In einem Grundzustand wird mittels Menü-Steuerung eines von acht Auswahl-Modulen angewählt. Dabei steht jedes Modul für einen speziellen Aktionstyp. In der folgenden Tabelle sind die Module und die entsprechenden Aktionen einander zugeordnet dargestellt:

10

Modul Nummer	Aktion
1	Öffnung einer Zugangsschleuse
2	Zahlung mit Kreditkarte
3	Zahlung mit Debitkarte
4	Übermittlung einer E-Banking Streichliste
5	Bargeldbezug am Geldautomaten
6	Erstellung eines Tickets im E-Ticketing
7	Übermittlung eines Zugriffs-Passwortes
8	E-Voting

Die Eingabe des ausgewählten Moduls wird mit einer PIN durch den Benutzer bestätigt.

15

Die Eingaben werden durch das Identifikationsmodul überprüft und bei Gültigkeit ein einmal gültiger TRX mit zeitlich begrenzter Gültigkeit generiert. Dieser TRX wird sowohl an den Benutzer als auch an die betreffende weitere Partei gesendet.

20

Bei falschen Eingaben des Benutzers oder Zeitüberschreitung bei der Eingabe wird von dem Mobiltelefon automatisch in den Grundzustand zurückgeschaltet.

25

Fig. 4 zeigt den weiteren Ablauf im Fall einer Zugangskontrolle nach Auswahl von Modul Nummer Eins. Nach Empfang des TRX mittels SMS-Nachricht von dem

5 Identifikationsmodul wird dem Benutzer dieser am Bildschirm des Mobiltelefons angezeigt. An der betreffenden Türe wird der TRX ebenfalls bereitgestellt.

Der Benutzer wählt auf seinem Mobiltelefon den empfangenen
 10 TRX aus und bestätigt diesen durch Eingabe einer Applikations-PIN. Dies wird dann - wiederum per SMS-Nachricht - an das Identifikationsmodul gesendet. Dort werden die Daten überprüft und bei Gültigkeit wird von dem Identifikationsmodul über eine GSM-Schnittstelle an ein
 15 Terminal, das mit der Türe verbunden ist, eine Nachricht gesendet, die wiederum ein Öffnen der Türe aktiviert.

Bei Eingabe von falschen Daten durch den Benutzer schaltet das Mobiltelefon automatisch in den Zustand zurück, in dem
 20 der TRX ausgewählt werden kann.

Fig. 5 zeigt den Ablauf im Fall einer Zahlung mit Kredit- oder Debit-Karte. Nach Empfang des TRX und eventuell eines vorgegebenen Maximalbetrages werden an der Kasse die Preise
 25 eingekaufter Artikel aufaddiert und von dem Kassenspersonal der - auch an der Kasse zur Verfügung stehende - TRX ausgewählt und die Summe dem TRX zugeordnet.

Zur Terminierung werden durch den Benutzer der betreffende
 30 Betrag zusammen mit dem TRX und einem Applikations-PIN freigegeben.

Nach Feststellung der Gültigkeit der Transaktionsfreigabe und des eingegebenen Applikations-PIN durch das
 35 Identifikationsmodul wird eine Quittung erstellt und die

Zahlung ist abgeschlossen. Ist die Prüfung negativ, muss die Eingabe wiederholt werden.

Die Kassendaten werden gesammelt und zu einem späteren
5 Zeitpunkt zur Weiterverarbeitung übermittelt.

Fig. 6 zeigt den weiteren Ablauf im Falle von Modul Vier, Streichliste für E-Banking. Nach Empfang des TRX mittels SMS-Nachricht gibt nun der Benutzer in eine Login-Maske auf
10 seinem mit dem Internet verbundenen PC außer seiner User-ID den TRX und eine PIN zur Terminierung ein.

Bei korrekter Eingabe wird die E-Banking-Applikation gestartet. Andernfalls muss der Ablauf wiederholt werden.
15

Fig. 7 zeigt den weiteren Ablauf im Falle von Modul Fünf, Bargeldauszahlung am Geldautomaten. Nach Empfang des TRX mittels SMS-Nachricht öffnet sich der Geldautomat automatisch. Daraufhin bestätigt der Benutzer den
20 bereitstehenden TRX mittels Eingabe einer Applikations-PIN an der Tastatur des Geldautomaten.

Anschließend kann die gewünschte Stückelung eingegeben werden.
25

Bei korrekter Eingabe wird der gewünschte Geldbetrag ausbezahlt.

Fig. 8 zeigt den weiteren Ablauf im Falle von Modul Nummer
30 Sechs, E-Ticketing im Fernverkehr Nach Empfang des TRX mittels SMS-Nachricht gibt nun der Benutzer am Terminal des Schaffners zur Bestätigung der Transaktion eine Applikations-PIN ein. Wiederum wird die Eingabe automatisch überprüft und bei positiver Rückmeldung wird eine Quittung
35 und ein Ticket ausgedruckt.

Andernfalls muss der Ablauf wiederholt werden.

Fig. 9 zeigt den weiteren Ablauf im Falle von Modul Nummer

-
- 5 Sieben, Zugriffskontrolle. Nach Empfang des TRX mittels SMS-Nachricht gibt nun der Benutzer in eine Einstiegs-Maske auf seinem mit dem Internet verbundenen PC außer seiner User-ID den TRX und eine PIN zur Terminierung ein.
- 10 Bei korrekter Eingabe wird die betreffende Applikation gestartet. Andernfalls muss der Ablauf wiederholt werden.

Die Vorteile des erfindungsgemäßen Verfahren lassen sich
15 wie folgt zusammenfassen:

- An die weitere Partei, die neben dem Benutzer an der Aktion beteiligt ist, werden keine sicherheitsrelevanten Daten des Benutzers geleitet. Dennoch kann die Aktion
20 unter besonders hoher Sicherheit durchgeführt werden.
 - Durch einen TRX, der einerseits zeitlich limitiert ist und andererseits nur einmal (oder begrenzt oft) gültig ist, wird der Sicherheitsfaktor entscheidend erhöht.
 - Der Ablauf einer Aktion kann durch die erfindungsgemäße
25 Untergliederung des Verfahrens in „Vorausisierung“ und „Terminierung“ beschleunigt werden, denn eine
-
- Zahlungsaktion kann bereits initialisiert werden, bevor von einer Scannerkasse der entsprechende Betrag zum Zahlungsterminal übermittelt worden ist.
- 30 • Es sind sehr viele unterschiedliche Terminaltypen erfindungsgemäß ansteuerbar, da die Ansteuerung über eine Luftschnittstelle erfolgt.
 - Bei der Durchführung einer Wahl kann durch die
35 ortsunabhängige und zeitlich besonders flexible Gestaltungsmöglichkeit einer Stimmabgabe eine Zunahme der

Wahl- beziehungsweise Abstimmungsbeteiligung erwartet werden.

Bezugszeichenliste

1	Benutzer eines Mobilterminals / Mobiltelefons
2	Identifikationsmodul / Server eines
5	Identifikationsmoduls
3	dritte Partei / (Aktions-)Terminal der dritten Partei
5	Anforderung einer TRX durch den Benutzer
6	Generierung einer TRX
7	Übersendung der TRX an das Mobiltelefon und (optional)
10	auch an die dritte Partei
8	Übersendung der TRX und einer PIN an das
	Identifikationsmodul
8'	Übersendung der TRX und einer PIN an die dritte Partei
10	Vorauthorisierung
15	20 Terminierung
50	Anforderung einer TRX für ein Download von
	Abstimmungsunterlagen
60	Generierung einer TRX für ein Download von
	Abstimmungsunterlagen
20	70 Übersendung der TRX für ein Download von
	Abstimmungsunterlagen an das Mobiltelefon und
	an die Wahl-Behörde
80	Terminierung des ersten Download-Teils
500	Anforderung einer TRX für eine Stimmabgabe
25	600 Generierung einer TRX für eine Stimmabgabe
700	Übersendung der TRX für eine Stimmabgabe an das
	Mobiltelefon und an die Wahl-Behörde
800	Terminierung des Stimmabgabe-Teils

Ansprüche

1. Verfahren zur Generierung einer Aktionsberechtigung für
einen Benutzer (1) eines Mobilterminals unter
5 Zuhilfenahme eines Mobilterminals, insbesondere eines
Mobiltelefons oder eines „Personal Digital Assistant“
(PDA) und eines Identifikationsmoduls,
aufweisend folgende Schritte:
 - a) Übersendung (5) einer Aktionsberechtigungs-
10 Anforderung über eine Luftschnittstelle von dem
Mobilterminal an das Identifikationsmodul (2),
 - b) Generierung (6) einer Aktions-Codenummer durch das
Identifikationsmodul (2),
 - c) Übersendung (7) der Aktions-Codenummer über die
15 Luftschnittstelle von dem Identifikationsmodul (2) an
das Mobilterminal,
 - d) Übersendung (8) einer persönlichen
Identifikationsnummer von dem Mobilterminal über eine
Luftschnittstelle an das Identifikationsmodul (2) oder
20 von einem Sendegerät über ein Telekommunikations-
Netzwerk an ein Aktionsterminal (3), um die durch die
Aktions-Codenummer spezifizierte Aktionsberechtigung zu
aktivieren,
dadurch gekennzeichnet,
25 dass die Gültigkeit der Aktions-Codenummer zeitlich
begrenzt ist.
2. Verfahren nach Anspruch 1,
dadurch gekennzeichnet,
30 dass die maximale Anzahl der Aktionsberechtigungen für
die eine Aktions-Codenummer gültig ist, beschränkt ist.
3. Verfahren nach Anspruch 1 oder 2,
dadurch gekennzeichnet,
35 dass mittels des Aktionsterminals (3) Vorgänge

auslösbar sind, die zur Durchführung der Aktion, auf die sich Schritt a) bezieht, notwendig sind.

-
4. Verfahren nach einem der Ansprüche 1 bis 3,
5 dadurch gekennzeichnet,
dass es sich bei dem Sendegerät um einen Computer handelt.
5. Verfahren nach einem der Ansprüche 1 bis 4,
10 dadurch gekennzeichnet,
dass es sich bei dem Telekommunikations-Netzwerk um das Internet handelt.
6. Verfahren nach einem der Ansprüche 1 bis 5,
15 dadurch gekennzeichnet,
dass durch Schritt d) die Terminierung der Aktion, auf die sich Schritt a) bezieht, ausgelöst wird.
7. Verfahren nach einem der Ansprüche 1 bis 6,
20 dadurch gekennzeichnet,
dass die Kommunikation zwischen dem Mobilterminal und dem Identifikationsmodul (2) zumindest teilweise mittels eines Datenkanals, wie zum Beispiel einer SMS-Nachricht des GSM-Standards erfolgt.
- 25 8. Verfahren nach einem der Ansprüche 1 bis 7,
dadurch gekennzeichnet,
dass bei der Kommunikation zwischen dem Mobilterminal und dem Identifikationsmodul (2) aus einem Speicher in
30 dem Mobilterminal ausgelesene Daten verwendet werden.
9. Verfahren nach Anspruch 8,
dadurch gekennzeichnet,
dass die Daten aus einer in das Mobilterminal
35 eingesetzten Karte mit Speicherfunktion ausgelesen
-

werden.

10. Verfahren nach einem der Ansprüche 1 bis 9,
dadurch gekennzeichnet,
5 dass die Kommunikation zwischen dem Mobilterminal und dem Identifikationsmodul (2) verschlüsselt erfolgt.
11. Verfahren nach einem der Ansprüche 1 bis 10,
dadurch gekennzeichnet,
10 dass Informationen bezüglich der Aktion, auf die sich Schritt a) bezieht, in einem Speicher des Mobilterminals abgelegt werden.
12. Verfahren nach Anspruch 11,
15 dadurch gekennzeichnet,
dass die Informationen durch einen autorisierten Benutzer des Mobilterminals ausgelesen und/oder zu einem anderen Gerät übertragen werden.
- 20 13. Verfahren nach einem der Ansprüche 1 bis 12,
dadurch gekennzeichnet,
dass es sich bei der Aktion um einen Zahlungsvorgang handelt.
- 25 14. Verfahren nach einem der Ansprüche 1 bis 13,
dadurch gekennzeichnet,
dass es sich bei dem Aktionsterminal (3) um ein Terminal eines Zahlungsadressaten handelt.
- 30 15. Verfahren nach einem der Ansprüche 1 bis 14,
dadurch gekennzeichnet,
dass mittels des Aktionsterminals (3) ein Vorgang in einer Kasse auslösbar ist.
- 35 16. Verfahren nach einem der Ansprüche 1 bis 15,

dadurch gekennzeichnet,
dass mittels des Aktionsterminals (3) ein Vorgang in
einem Geldautomaten auslösbar ist.

-
- 5 ~~17. Verfahren nach einem der Ansprüche 1 bis 16,~~
dadurch gekennzeichnet,
dass mittels des Aktionsterminals (3) eine
verschießbare Türe geöffnet werden kann.
- 10 18. Verfahren nach einem der Ansprüche 1 bis 17,
dadurch gekennzeichnet,
dass mittels des Aktionsterminals (3) ein Ticket
ausgedruckt werden kann.
- 15 19. Verfahren nach einem der Ansprüche 1 bis 18,
dadurch gekennzeichnet,
dass es sich bei der Aktion um eine Stimmabgabe einer
Wahl handelt.
-
-

20. Verfahren zur Identifizierung eines Benutzers (1) eines Mobilterminals gegenüber einem Identifikationsadressaten unter Zuhilfenahme eines Mobilterminals, eines davon unabhängigen Identifikationsmoduls (2) und eines Terminals (3) des Identifikationsadressaten, aufweisend folgende Schritte
- a) Übersendung (5) einer Identifizierungs-Anforderung von dem Mobilterminal an das Identifikationsmodul (2),
 - b) Generierung (6) einer Berechtigungs-Codenummer durch das Identifikationsmodul (2),
 - c) Übersendung (7) der Berechtigungs-Codenummer von dem Identifikationsmodul (2) an das Mobilterminal,
 - d) Übersendung (7) der Berechtigungs-Codenummer von dem Identifikationsmodul an das Aktionsterminal (3),
 - e) Übersendung (8) einer persönlichen Identifikationsnummer von dem Mobilterminal an das Identifikationsmodul (2) oder von einem Sendegerät eines Telekommunikations-Netzwerkes an das Terminal (3) des Identifikationsadressaten, um die durch die Berechtigungs-Codenummer spezifizierte Identifizierungs-Anforderung zu aktivieren, dadurch gekennzeichnet, dass die Übersendungen an das Terminal (3) des Identifikationsadressaten wenigstens teilweise über eine Luftschnittstelle erfolgen, mittels der das Terminal (3) des Identifikationsadressaten drahtlos adressierbar ist.
21. Verfahren nach Anspruch 20, dadurch gekennzeichnet, dass die Gültigkeit der Identifizierungs-Codenummer zeitlich begrenzt ist.
22. Verfahren nach Anspruch 20 oder 21,

dadurch gekennzeichnet,
dass die Identifizierungs-Codenummer nur einmal oder
begrenzt oftmals gültig ist.

5 23. Verfahren nach einem der Ansprüche 20 bis 22,
dadurch gekennzeichnet,
dass mittels des Terminals (3) Vorgänge auslösbar sind,
die zur Durchführung der Aktion, auf die sich Schritt
a) bezieht, notwendig sind.

10

24. Verfahren nach einem der Ansprüche 20 bis 23,
dadurch gekennzeichnet,
dass es sich bei dem Sendegerät um einen Computer
handelt.

15

25. Verfahren nach einem der Ansprüche 20 bis 24,
dadurch gekennzeichnet,
dass es sich bei dem Telekommunikations-Netzwerk um das
Internet handelt.

20

26. Verfahren nach einem der Ansprüche 20 bis 25,
dadurch gekennzeichnet,
dass durch Schritt d) die Terminierung der Aktion, auf
die sich Schritt a) bezieht, ausgelöst wird.

25

27. Verfahren zur Identifizierung eines Benutzers (1) eines Mobilterminals gegenüber einem Identifikationsadressaten unter Zuhilfenahme eines Mobilterminals, eines davon unabhängigen Identifikationsmoduls (2) und eines Terminals (3) des Identifikationsadressaten, aufweisend folgende Schritte
- a) Übersendung (5) einer Identifikations-Anforderung von dem Mobilterminal über eine Luftschnittstelle an das Identifikationsmodul (2),
 - b) Generierung (6) einer Identifizierungs-Codenummer durch das Identifikationsmodul (2),
 - c) Übersendung (7) der Identifizierungs-Codenummer von dem Identifikationsmodul (2) über eine Luftschnittstelle an das Mobilterminal,
 - d) Übersendung (7) der Identifizierungs-Codenummer von dem Identifikationsmodul (2) über eine Luftschnittstelle an das Terminal (3),
 - e) Übersendung (8) einer persönlichen Identifikationsnummer von dem Mobilterminal an das Identifikationsmodul (2) oder von einem Sendegerät eines Telekommunikations-Netzwerkes an das Terminal (3) des Identifikationsadressaten, um die durch die Identifizierungs-Codenummer spezifizierte Identifizierungs-Anforderung zu aktivieren, dadurch gekennzeichnet, dass die Gültigkeit der Identifizierungs-Codenummer zeitlich begrenzt ist.
28. Verfahren nach Anspruch 27, dadurch gekennzeichnet, dass die Identifizierungs-Codenummer nur einmal oder begrenzt oftmals gültig ist.

29. System zur Identifizierung eines Benutzers (1) eines Mobilterminals nach einem der Ansprüche 1 bis 28, aufweisend ein Mobilterminal, ein Identifikationsmodul (2) und ein Aktionsterminal (3),

5 dadurch gekennzeichnet,
dass die Kommunikation zwischen dem Mobilterminal und dem Identifikationsmodul (2) und zwischen dem Identifikationsmodul (2) und dem Aktionsterminal (3) jeweils über eine Luftschnittstelle erfolgt.

10

30. Mobilterminal, programmiert zur Durchführung eines Verfahrens nach einem der Ansprüche 1 bis 28,

15

31. Identifikationsmodul (2), programmiert zur Durchführung eines Verfahrens nach einem der Ansprüche 1 bis 28,

32. Aktionsterminal (3), programmiert zur Durchführung eines Verfahrens nach einem der Ansprüche 1 bis 28,

20

33. Software-Programm,
dadurch gekennzeichnet,
dass es die Implementierung eines Verfahrens nach einem der Ansprüche 1 bis 28 ermöglicht.

25

Zusammenfassung

Es wird eine Verfahren vorgestellt, mit dem ein Benutzer
(1) eines Mobilterminals, insbesondere eines Mobiltelefons
5 oder eines PDA identifiziert werden kann und diesem
Benutzer (1) eine Berechtigung für eine Aktion erteilt
werden kann. Dazu dient ein unabhängiger
Identifikationsserver (2). Von dem Benutzer wird zunächst
eine Anforderung für eine Identifizierung / Berechtigung
10 über eine Luftschnittstelle, beispielsweise per SMS-
Nachricht an den Identifikationsserver (2) gesendet. In
diesem wird eine Code (TRX) erzeugt, der einmalige
Gültigkeit besitzt und außerdem nur zeitlich begrenzt
gültig ist. Dieser TRX wird von dem Identifikationsserver
15 sowohl an den Benutzer (1) des Mobilterminals, als auch an
einen Server der an der Aktion beteiligten dritten Partei
(3) gesendet. Beispiele für die dritte Partei (3) sind:
Supermarkt, Zutrittsschleuse, Bank oder Wahlbehörde. Die
Durchführung der gewünschten Aktion, beispielsweise
20 Zahlung, Zutritt durch eine Schleuse, E-Banking oder
Stimmabgabe bei einer Wahl, kann durch den Server der
dritten Partei initialisiert werden. Zur Terminierung
sendet der Benutzer (1) eine PIN an den
Identifikationsserver (2) oder direkt an die dritte Partei
25 (3).

30. Juli 2002

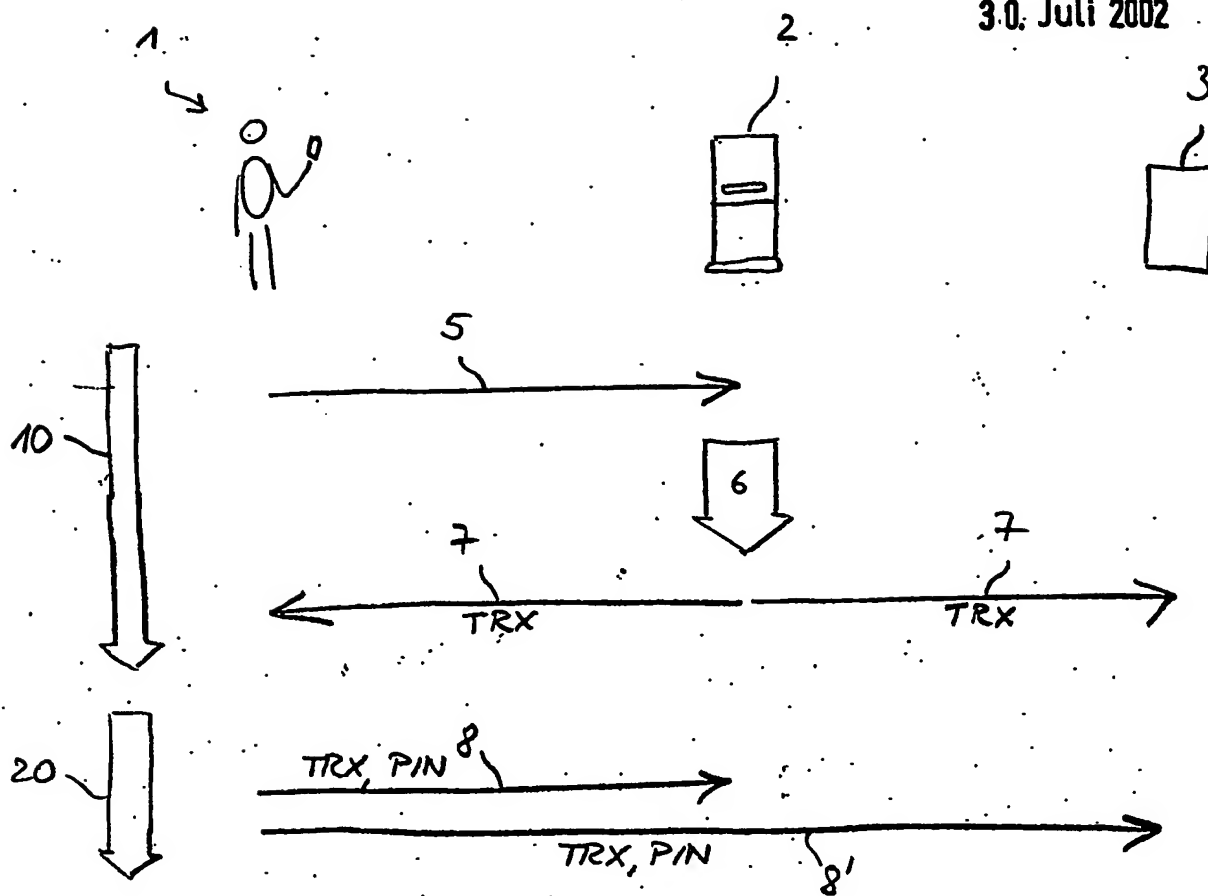


Fig. 1

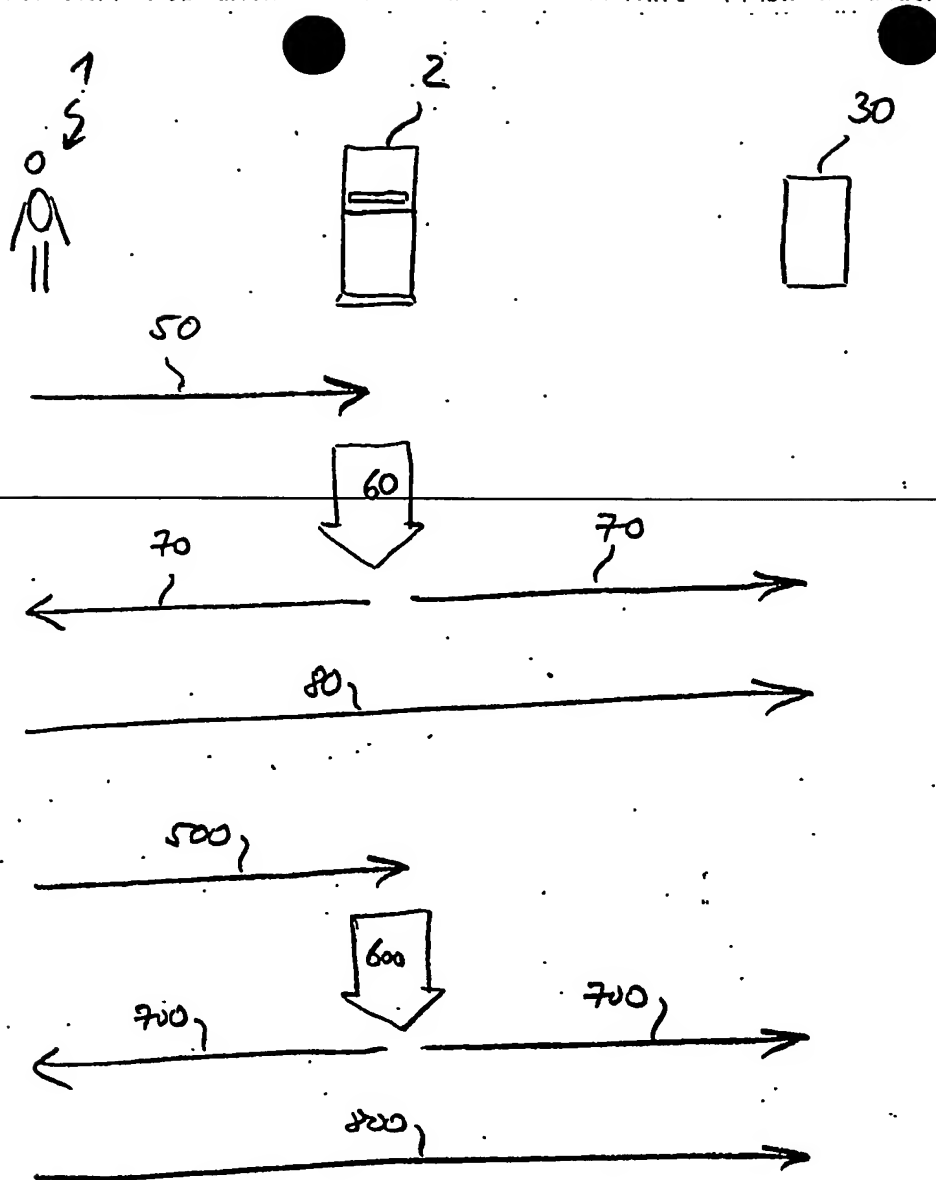


Fig. 2

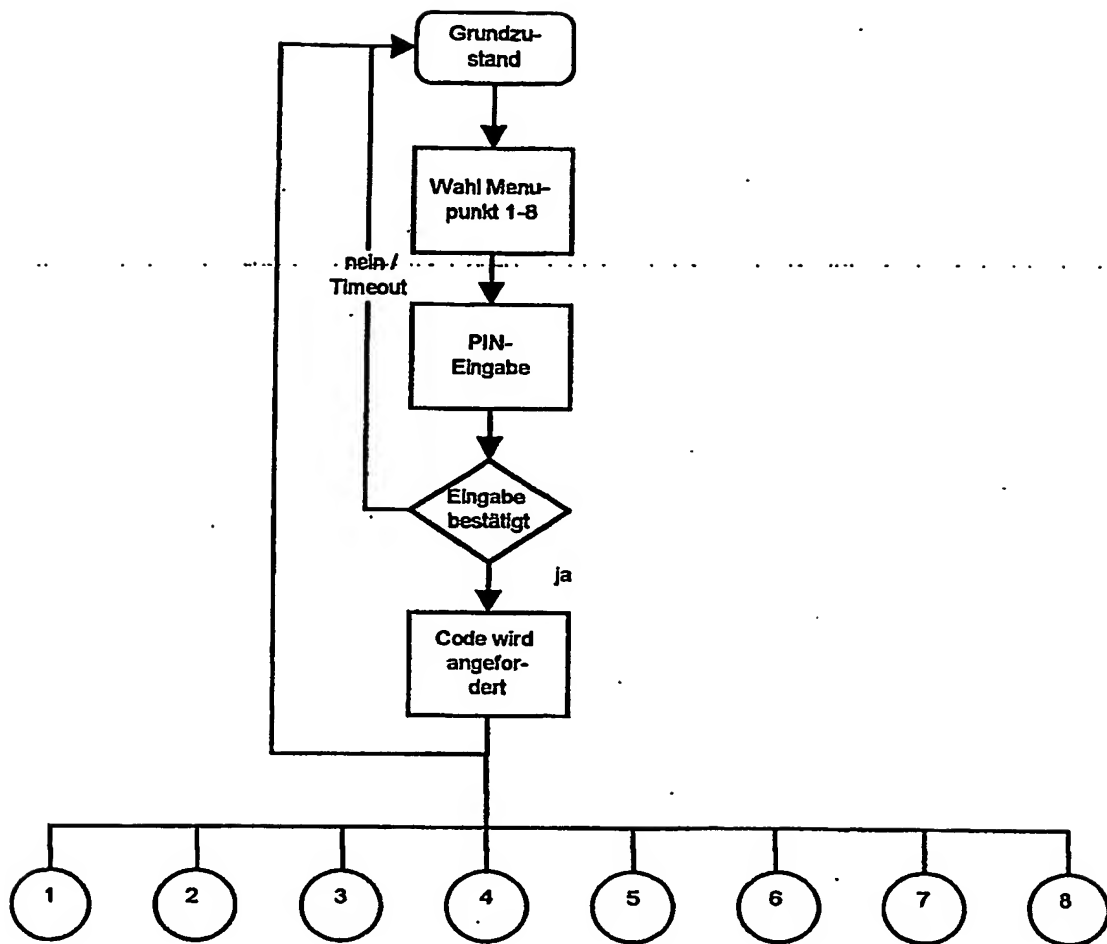


Fig. 3

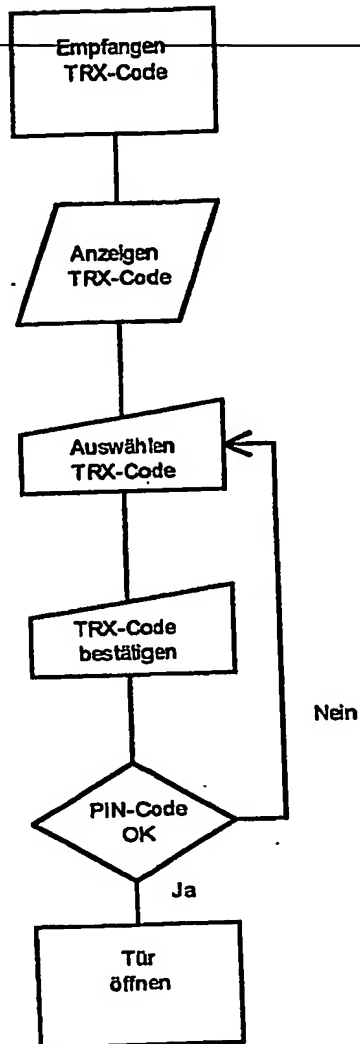


Fig. 4

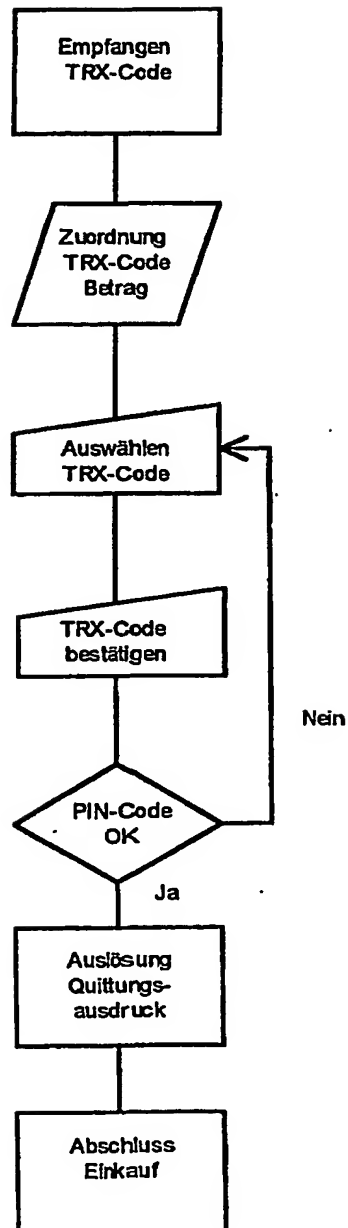


Fig. 5

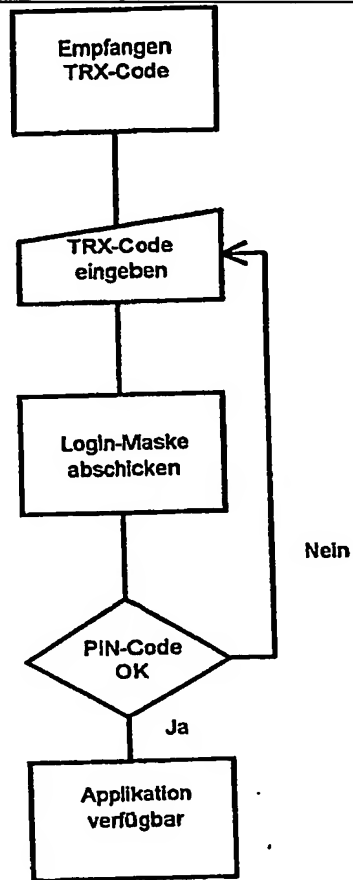


Fig. 6

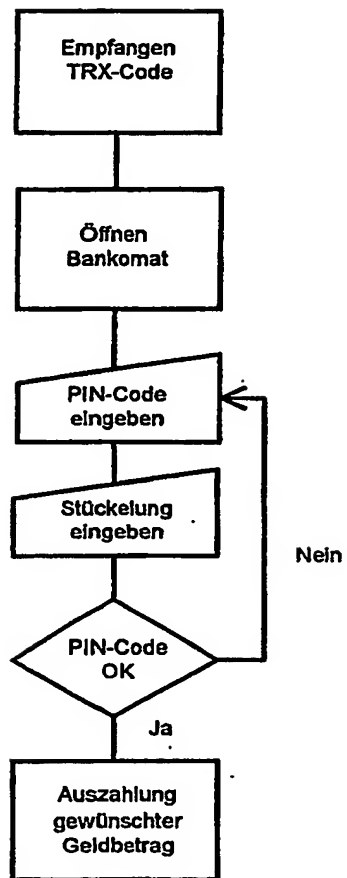


Fig. 7

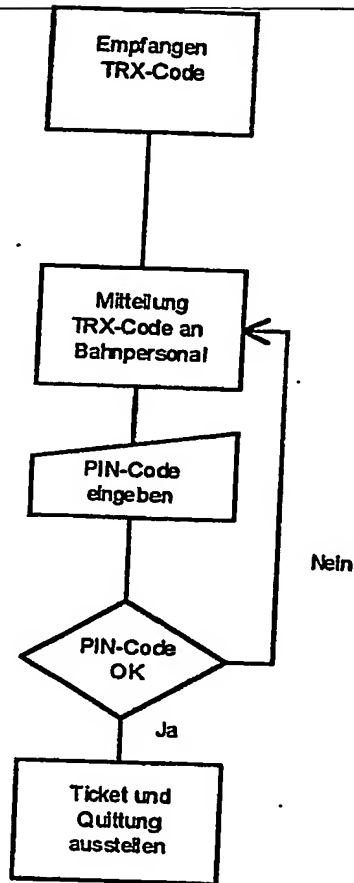


Fig. 8

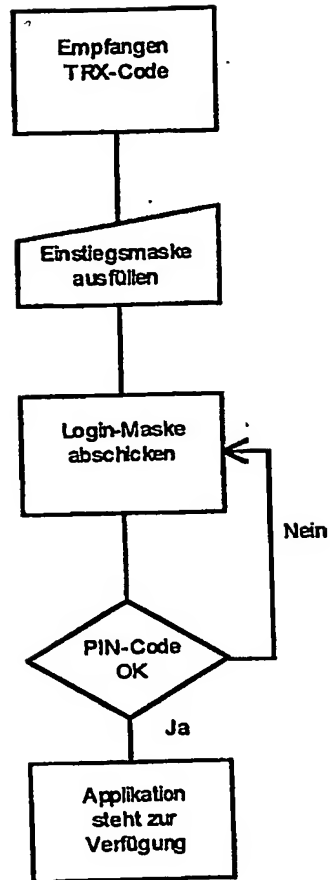


Fig. 9

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.